From History of cryptography

Stanislav Palúch

University of Žlina/Department of Mathematical Methods

9. októbra 2017

Oldiest Historical Sources

1900 before Christ, a master scribe used some unusual hieroglyphic symbols that told the story of his lord's life. This was not a secret writing in our modern sence. However the scribe substituted known hieroglyphs by another ones.
Egyptian scribes were often replacing the usual hieroglyphic form of a letter by a different form. Sometiemes they used new hieroglyphs. Such writings can be found on tombs of venerated dead. [Kahn sp. 71]

1500 B.C – Mesopotamia
A tiny cuneifor tablet only about 7.5 by 5cm B.C was found on the site of ancients Seleucia on the banks of Tigris from bove 1500 B.C. It contains the earliest known formula for making of glazes o pottery. It's author evidently tried to guard his professional secrects by several ways. [Kahn str. 75]

Oldiest Historical Sources

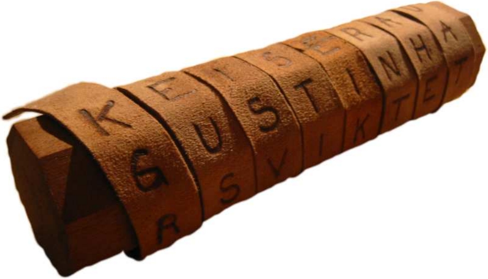
cca 500 B.C. -Greece -Persia
One Histiaeus, wanting to send a message from the Persian court to his son-in-law Aristagoras in Miletus, shawed the head of a slave, tattooed the secred message on his head, waited for a new hair to grow and sent the slave to his son-in-law with the instruction to shave the slave's head. So Aristagoras received a message that uged him to revolt against Persia.

600 - 500 B.C. – Ancient Israel
Hebrews used a primitive transformation of letters called „atbash", wher first leetter in hebrew alphabet was replaced by last, second by last but one, ets. In several places it was used without any aparent desire to conceal. Several application of atbash can be found in Holy Scriptures - Old Testament where for example BABEL is replace by SHESHACH.

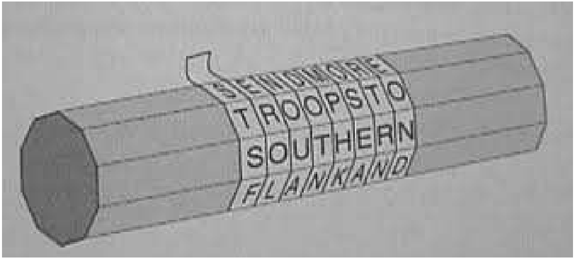
Hebrews used (besides) atbash two similar ways called „atbam" and „atbah". The last mentioned system replaced first nine letters by shifting them ten positions. What happens to 19-th and those byond is not clear. [Kahn str. 82]

Greece and Sparta

500 pred B.C.
Spartans established the first system of military cryptography called skytale. Skytale was staf of wood around which a strip of papyrus or leather is wrapped. The secret message is writen on the papyrus or lether strip down the length of the staf. The strip is then unwound and sent to recipient. Recipient rewraps the strip around a staf with the same diameter as the one of sender and now can read message.



Greece and Sparta



Greece and Sparta

First instructional text on communication security appeared as an entire chapter in one of the earliest works on military science – On the Defencse of Fortified Places by Aeneas the Tactician.
Aeneas suggested maybe the first method of steganography – pricking holes in a book or other document above or below the letters of the secret message. German spies used this method in World War I. and World War II. by dotting letter with invisible ink.

Another Greek writer, Polyobius devised a system of signaling that has been adopted as a cryptographic method. He arranged letters of alphabet into a 5x5square

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	ij	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Each letter can now be represented as a couple of two numbers. This system was originaly created for signaling by two torches – one in left and one in right hand.

Ceasar cipher

100 - 44 B.C Julius Ceasar

Julius Ceasar used a cipher that replaced every letter by the letter shifted three positions rearwords.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

C	E	A	S	A	R
F	H	D	V	D	U

Ceasar employed cryptografy habitually[a] and not only on single isolated situations.

His cipher was unsolvable in his days, untill his former friends (Cicero) unveiled it after they came to his enemies.

[a] zo zvyku, obvykle

India and Arab Roots of Cryptography

Between 1. - 4.
Kámasútra presents as 44-th art of lovers:
To understand writing of ciphers and words to conceal affairs.

725-790
Abu Abd al-Rahman al-Khalil ibn Ahmad ibn Amr ibn Tammam al Farahidi al-Zadi al Yahmadi
wrote a book on cryptography. This book was inspired by his experiences gained by breaking ciphers for Byzantine emerator.
His methodology is based on knowledge of properties a of language, what is standard cryptography method used till our days.

Another Arab cryptologist Ibn ad-Duranhim wrote:
When you want to solve a message which you have received in code you must know the language in which the message is written. First of all begin by counting the letters. ...
He evidently uses frequency analysis which is till sry strong cryhptographic tool.

Italy and Venecia

1226 n.l.
Arhives of Venice show that in some documents dots and crosses replaced letters the vowels[1] in some scattered[2] words.

The oldest cryptographic document in Vatican (1327) contains a list of name-equivalents for use in the struggle between the pro-pope[3] Guelphs and the pro-Holy Roman Emperore Ghibellnes in central Italy.

[1] samohlásky
[2] roztrúsený
[3] pápežovi oddaný

Gabrieli di Lavinde

In 1378 Great Schizm of the Roman Catholic Church began, in which two popes claimed to reign. Antipope Clement VII fled to Avignon (1378). Gabrieli di Lavinde was one of his secretaries.

Gabrieli di Lavinde created a system cosisting of complete substitution alphabet extended by two-letter codes for cca two dozens common wordes and names.
Moreover, he created groups of letters without any real contence inorder to deceive potential analyst.

This principle have been used for more then 450 years despite existence of more poweful methods.

Remark.
Many cryptographic systems at that time used so called "dictionaries"containing codes – enciphered equivalents for several most common words.
One problem with such encoding schemes is that they rely on humanly-held secrets which disclose for example, the secret meaning of words in ciphertext.
Dictionaries, once revealed, permanently compromise a corresponding encoding system.

Leon Battista Alberti (1404-1472)

Leon Battista Alberti
was an Italian humanist author,
artist, architect, poet, priest,
linguist, philosopher and cryptographer;

Leon Batista Alberti has written a work having 25 pages (1466-1467) devoted to cryptoanalysis.
This was the first paper of this type written in west Europe.
The publication contains explanation of cryptonalalysis procedures on the basis of knowledge of language.
Moroeover Alberti propozes classification of cipher systems to substitution and transposition.
He also disovered polyalphabetical substitution and ciphering of codes.

Giovani Soro (? – 1544)– Venice

The Council of Ten – the poweful and misterious body ruled the Republic Venice from 1310 to 1797, largely through it's efecient secret police.

Giovani Soro was appointed cipher secretary in 1506.

He enjoyed remarkable success in solving the ciphers of numerous principalities[4].

He solved a dispatch of Marh Anthony Colonna (chief of the army of the Holy Roman Emperore Maximilian I) which revealed Colonna'sproblems.

He was able to break almost every contemporary cipher. Thats why many courts sharpened their ciphers.

It is known that Soro has written a book of cryptography on the solution of Latin, Italian Spanich and French ciphers, but it is lost – no trace of it can be found in archives.

[4] kniežatstvo, riaditeľstvo

Johannes Trithemius (1462 – 1516)

Was a German Benedictine abbot[a] and a polymath[b] active in the German Renaissance[c] as a lexicographer, chronicler, cryptographer and occultist.

1518 – Johannes Trithemius issued first printed book on cryptographypy.
He studied many aspects of cryptography and designed several ciphers

He proposed so called Trithemius table.
He enciphered first letter with first letter of plaintext with first letter of alphabet, the second letter with the second letter of alphabet and so on.

[a] mních – opát

[b] vševed, človek so všestrannými znalosťami

[c] renesancia

Johannes Trithemius (1462 – 1516)

POLYGRAPHIAE
LIBRI SEX, IOANNIS TRITHEMII AB
BATIS PEAPOLITANI, QVONDAM
SPANHEIMENSIS, AD MAXI-
MILIANVM CAESAREM.

Cum gratia et privilegio C. M.

IO. TRITHEMIVS

Trithemiusova tabuľka

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	J	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	A

A

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	J	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	A

$$\mathrm{T} + \mathrm{M} \to \mathrm{F}$$

Giovan Batista Belaso (1505 – ?)

1553 n.l. Giovan Batista Belaso was an Italian aristocrat.

In 1550 he was in the service of Cardinal Duranti in Camerino and had to use secret correspondence in the state affairs while his master was in Rome for a conclave.

Versed[5] in research, able in mathematics, Bellaso dealt with secret writing at a time when this art enjoyed great admiration in all the Italian courts, mainly in the Roman Curia.

His cipher marked an epoch and was considered unbreakable for four centuries.

His enciphering reciprocal table was circulating in loose-leaf form[6], in print and manuscript. The table was to be duly[7] completed with the instructions.

Copies of these tables exist in contemporary private collections in Florence and Rome.

[5] skúsený

[6] s voľnými listami

[7] riadne

Giovan Batista Belaso (1505 – ?)

1553 – Giovan Batista Belaso published a booklit
"La cifra"describing a cyptosystem based on so called
„secret code“

Secret code is here a word or a sentence, which is repeatidly written above letters of plaintext.

Every letter of plaintext is then enciphered by the row of Trithemius table determined by the letter above.

(Cipher based on this principle is wrongly arrogated[8] to Vigenèr.)

[8] pripisovať (aj neprávom)

Blaise de Vigenère (1523 – 1596)

Blaise de Vigenère gained classical education in Paris – he studied Greek and Hebrew.
At age 17 he entered the diplomatic service and remained there for 30 years.
Five years into his career he accompanied the French envoy Louis Adhémar de Grignan to the Diet of Worms as a junior secretary.
At age 24, he entered the service of the Duke of Nevers as his secretary, a position he held until the deaths of the Duke and his son in 1562.

BLAISE DE VIGENERE BOVRBONOIS. EN·LAGE·DE·LXXIII·ANS·1595.
DEVS NOBIS HÆC OTIA FECIT
ET. ERVNT.
VT. COMPLACEANT.
VERBA. ELOQVII. MEI.
Pſalm. 18.
Tho. de leu fe

Blaise de Vigenère (1523 – 1596)

He also served as a secretary to Henry III.

In 1549 he visited Rome on a two-year diplomatic mission, and again in 1566.

On his two diplomatic mission to Rome in 1549 and again in 1566 he read books about cryptography and came in contact with cryptologists.

After his retirement, Vigenér composed and translated over twenty books, including a book „Traicté des Chiffres“ (1856).

One of studied systems is so called "Vigenére cipher". The secret key is a word which is repeatedly written over letters of plaintext. Every letter of message is then enciphered by Ceasar cipher bye corresponding letter above.
For three centuries Vigenére cipher resisted all attempts to break it; this earned it the description „the indecipherable cipher“.
Friedrich Kasiski was the first to publish a general method of deciphering a Vigenčre cipher in 1863.

Blaise de Vigenère (1523 – 1596)

The method was originally described by Giovan Battista Bellaso in his book La cifra del. Sig. Giovan Battista Bellaso; however, the scheme was later misattributed to Blaise de Vigenére in the 19th century, and is now widely known as the "Vigenére cipher".

In book „Traicté des Chiffres“ (from 1586) in which (in addition to other ideas he proposes) a cipher in which the message itself is the key.

S	V	J	E	D	N	O	M	J	E	J	P	O	U	Z	I	T	I	P	O	S	T	U	P	U	J
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
v	j	e	d	n	o	m	j	e	j	p	o	u	z	i	t	i	p	o	s	t	u	p	u		
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	
N	E	N	H	Q	B	A	V	N	N	Y	D	I	T	H	B	B	X	D	G	L	N	J	J		

Example from
Grošek, O, Porubský, Š: Šifrovanie. Algoritmy, metódu, prax. 1992 - Grada.
ISBN 80-85424-62-2

Mary Stuart (1542 – 87) and Elizabeth I (1533 – 1603).

Elizabeth Tudor was qeen of England, Mary Stuart was qeen of Scots.

Mary (and her catholic supporters) also claimed Elizabeth's throne as her own.

Following an uprising against Mary and her husband, Elisabeth imprisoned Mary in 1568 and had her executed in 1587.

In 1586 it seamed that there was an occasion to organize a plot against Elizabeth.

Mary and her secretary Babington communicated with plotters through Gilbert Gifford who was a double-agent.

Encifered letters come to Thomas Phellipes, cryptoanalytic who succesfuly solved them. He even succeed to forge the letter from 17.july 1586 – he asked for „*the names and qualities of the six gentlemen which are to acomplish the designment*[9] ".

Next year 1587 Elizabeth had Mary executed.

[9] plán, cieľ, úmysel

FRANCE – Francois Viète (1540-1603)

Francois Viète – lawyer and matematician.

He was the first to use letters instead of numbers in mathematic calculations and equations.

He is considered as the founder of modern algebra.

He is one of the first mathematicians engaged in ciphering services.

He served as a privy councillor[a] to both Henry III and Henry IV of France.

In 1589, Henry III took refuge in Blois. He commanded the royal officials to be at Tours before 15 April 1589. Viéte was one of the first who came back to Tours. He deciphered the secret letters of the Catholic League and other enemies of the king.

[a] tajný radca

FRANCE – Antoine Rossignol (1599 - 1682)

Antoine Rossignol – French mathematician.
In april 19, 1628 french town Réalmont was under siege of royal army. Hugenots inside were putting up a stiff defence. The same day the soldiers captured an inhabitant of the town, who was trying to carry an enciphered message to Hugenot forces outside. No one of royal men could unriddle[a] it, but someone suggested to pass it to a young man – A. Rossignol – who was known to have an interest in ciphers.

[a] rozlúštiť

Antoine Rossignol
Mre. des Comptes.
alamy stock photo
D8C98J
www.alamy.com

He solved it at a spot. The message revealed that the Hugenots desperately needed munition and help. Royalists sent the solved message to Hugenots who after receiving it suddenly capitulated.
Later A. Rossignol become fundamental member of cipher office of cardinal Richelieu and cardinal Mazarin.

sir Francis Bacon (1561 – 1626)

Sir Francis Bacon was an English philosopher, statesman, scientist, jurist, orator, and author.
He served both as Attorney General and as Lord Chancellor of England.
He designed in his scientific work "De Augmentis Scientarum"(1623) a biliteral cipher which is known as 5-bit coding in present days.

A aaaaa	B aaaab	C aaaba	D aaabb	E aabaa	F aabab
G aabba	H aabbb	I abaaa	K abaab	L ababa	M ababb
N abbaa	O abbab	P abbba	Q abbbb	R baaaa	S baaab
T baaba	V baabb	W babaa	X babab	Y babba	Z babbb

Friedrich W. Kasiski (1805 – 1881)

Major Friedrich Wilhelm Kasiski was a German infantry officer, cryptographer and archeologist. Kasiski was born in Schlochau, Kingdom of Prussia (now Czluchów, Poland).

In 1863, Kasiski published a 95-page book on cryptography, Die Geheimschriften und die Dechiffrir-Kunst – German, "Secret writing and the Art of Deciphering".

This was the first published account of a procedure for attacking polyalphabetic substitution ciphers, especially the Vigenére cipher.

The significance of Kasiski's cryptanalytic work was not widely realised at the time, and he turned his mind to archaeology instead.

Historian David Kahn notes:
"Kasiski died on May 22, 1881, almost certainly without realizing that he had wrought a revolution in cryptology"

Auguste Kerckhoffs (1835 - 1903)

Auguste Kerckhoffs was a Dutch linguist and cryptographer who was professor of languages at the École des Hautes Études Commerciales in Paris in the late 19th century.

In 1883 he published a book: La Cryptografie militaire

Kerckhoffs' stated his principle:

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

He invented a method how to solve a polyalphabetic cipher with non periodic key provided that thi key i used several times.

Auguste Kerckhoffs (1835 - 1903)

He formulatedesix principles of practical cipher design:

1. The system must be practically, if not mathematically, indecipherable;
2. It should not require secrecy, and it should not be a problem if it falls into enemy hands;
3. It must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will;
4. It must be applicable to telegraph communications;
5. It must be portable, and should not require several persons to handle or operate;
6. Lastly, given the circumstances in which it is to be used, the system must be easy to use and should not be stressful to use or require its users to know and comply with a long list of rules.

Some of them became obsolet[10] but Kerkhoffs principle is stil valid and will be valid forever.

[10] zastaraly

Development of cryptography in 20. century

1919 – Hugo Alexander Koch patented his idea of enciphering machine based on rotors

1923 – Koch sold his patent to Arthur Scherbius, who enhanced machine and called it Enigma.

Enigma was used by german army during Worl War II.

1976 – Whitfield Diffie and Martin Hellman published
"New Directions in Cryptography"
introducing the notion of privite and public key (called also asymetrická cryptography).

1977 – Ronald L. Rivest, Adi Shamir a Leonard M. Adleman announced the invention of the first real cryptosyste with public key – RSA.

Development of cryptography in 20. century

in early 1970s – IBM developed symmetric cryptographic algorithm DES

1976 – after consultation with the National Security Agency (NSA), the National Bureau of Standards (NBS) eventually selected slightly modified version of DES as an official Federal Information Processing Standard (FIPS) for the United States in 1977.

1997 – The DESCHALL Project breaks a message encrypted with DES for the first time in public

1990 – Xuejia Lai a James Massey zo Švajčiarska published a paper "A Proposal for a New Block Encryption Standard", which contained design of algorithm International Data Encryption Algorithm (IDEA) which should replace DES.

1991 – Phil Zimmermann published his first version of PGP (Pretty Good Privacy). PGP je cryptographic system which can secure safe transfer of e-mail and morover telephon calls through Internet.

Latest Result of Cryptography

1994 – the number RSA-129 129-digit number was factorized.
This calculation should take 4.10^{16} years by former assessment of prof. Rivesta (one of investors of RSA).

2000 – encryption standard DES was repaced by belgian cipher Rijndael after 4-years long competition (Joan Daemen and Vincent Rijmen).

Cryptography

Cryptography je a study of mathematical techniques for secure communication and secresy of data.

Sometimes is used term Cryptologywhich cosists from

- Cryptography – designing enciphering systems and
- Cryptanalsis – studying attacks against enciphering systems.

Goals of cryptography

- Condifentiality of information
- Insuring of data integrity – securing against changes or forgering
- Autentification – securing that message comes from certain sender
- Identifikácia – securing that communication is with desired person
- Digitaln signature
- Steganography

Kryptografia

Further topics of cryptography

- Key exchange
- Key sharing
- Electronic money
- Anonymous voting procedures
- etc.

Cryptosystem

$$\boxed{\text{Plaintext}} \rightarrow \boxed{\text{ Ciphertext}}$$

A cryptosystem is a sorted quadrupleje $(\mathcal{K}, \mathcal{M}, \mathcal{C}, \mathcal{T})$ where

- $\mathcal{K}$ is a key set
- $\mathcal{M}$ is a set of plintezxts
- $\mathcal{C}$ is a set of cipher texts
- $\mathcal{T}$ is a mapping $\mathcal{T} : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$, which assignes a cipjertext $C \in \mathcal{C}$ to every couple $K \in \mathcal{K}$, $M \in \mathcal{M}$ such that

  if $\mathcal{T}(K, M) = C$ and $\mathcal{T}(K, M') = C$, then $M = M'$.

  (The exists an inversion mapping $\mathcal{T}^{-1}(K, C) = M$.)

We will write $\mathcal{T}(K, M) = E_K(M)$, $\mathcal{T}^{-1}(K, C) = D_K(C)$.

Types fo cryptography systems

- **Symetric cryptography** – the same key is used for enciphering and deciphering.
- **Aymetricá cryptography** – public key cryptography.
  So calle public key is used for enciphering. Recipient deciphers received message by his private – secret key.
  It is not possible to derive private key from publik key.
- **Substitution cipher** – it replaces letter or string of letters bye another letter resp. string.
- **Transposition cipher** – letters remain without changes, order of letter changes
- **Monoalfabetic cipher** – enciphers letter by letter, every letter changes using the same mapping zobrazením
- **Polyalfabetic cipher** – enciphersa k-tuples of letters, every letter in k-tuple by different key
- **Stream cipher** – enciphers letter by letter, every letter by another key, key stream has length equal to the one of enciphered message.

What remained from Kerckhoff's principles

1. Revelation of enciphering algorithm must not affect safety of cryptosystem.
2. Savety consists only in confidentiality of key.

Kryptografické útoky.

Cryptography attack is a procedure which reveals plaintext (or at leat a part of it) or even discovers used enciphering key.

Types cryptography attacks

- Brute force attack
- Ciphertext only attack
- Known plaintext attack
- Chosen plaintext attack
- Chosen ciphertext attack
- Dictionary attack
- Rubber hose attack